Reporting SSL Parameters in EDR

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	All Products supporting ADC
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	*ADC Administration Guide*

Revision History

Revision Details	**Release**
First introduced.	21.5

Feature Description

The ADC (P2P) engine detects encrypted traffic using Server Name Indication (SNI)/ Canonical Name (CNAME) field (signatures) of SSL flow in Client and Server Hello packets. To mark the flow as SSL, both Client and Hello packets must be parsed without any error. There could be several error conditions due to which ADC SSL decoder could fail, such as failure to receive Server Hello, invalid Type Value Length (TLV), invalid header length, absence of a certificate, and so on. When any of these error conditions are seen, the flow is marked as "p2p-unknown" instead of SSL although the packets are exchanged on TCP Port 443. As a result, the flow is matched to the "ip any-match" rule instead of an SSL rule.

With this feature, these failure reasons are reported in EDR for better debugging purposes and to know why a flow is not marked as SSL. Subsequently, marking a flow as an application traffic based on SNI has a limitation of users spoofing the SNI field to gain advantage of the various service provider monetary plans. SSL makes use of certificates to authenticate the endpoints. As such, to overcome SNI spoofing, ADC parses the various information in the SSL Server Hello packet and reports the same in EDR for debugging.

How It Works

This section provides a brief overview of how this feature works.

- ADC stores the reason for SSL decode failure.
- ADC stores the validity of SSL certificate.
  - Has the certificate expired (> not-after).
  - Is the certificate still valid (between not-before and not-after).
  - Can the certificate be used (< not-before).

    Currently, ADC decodes ‘not-after’ and ‘not-before’ and stores them internally. As part of this feature, the ‘not-after’ and ‘not-before’ is parsed with current system time and report values 0, 1, 2 in EDR.

- Support is added to configure the required SSL certificate parameters in EDR.
- Support is added to report the certificate information in charging EDR.
- Support is added to generate charging EDR for that flow and report the parsed information.
- Boxer is compatible with a plugin with and without changes.
- If the value of attributes; SSL ISSUER CNAME, SSL ISSUER ORG or SSL SUBJECT ORG contains “,”, the Boxer converts the same to “_” before printing in EDR.

EDR

The SSL parameters issued from plugin can be configured as EDR fields. The particular values corresponding to different EDR fields is populated, if present in the flow.

Following SSL parameters are identified to be reported in EDR:

- **SSL decode failure**: A flow can fail to be detected as SSL due to one of the following reasons:

1. IPOQUE_SSL_CLIENT_HELLO_DECODE_SUCCESS,
2. IPOQUE_SSL_SERVER_HELLO_DECODE_SUCCESS,
3. IPOQUE_SSL_CLIENT_HELLO_INVALID_EXT_LEN,
4. IPOQUE_SSL_SERVER_HELLO_INVALID_EXT_LEN,
5. IPOQUE_SSL_SERVER_HELLO_NO_CERTIFICATE,
6. IPOQUE_SSL_SERVER_HELLO_INVALID_SNO_LEN,
7. IPOQUE_SSL_SERVER_HELLO_INVALID_SIGNATURE_LEN,
8. IPOQUE_SSL_SERVER_HELLO_ISSUER_NOT_FOUND,
9. IPOQUE_SSL_SERVER_HELLO_INVALID_VALIDITY,
10. IPOQUE_SSL_SERVER_HELLO_INVALID_VALIDITY_NOT_BEFORE,
11. IPOQUE_SSL_SERVER_HELLO_INVALID_VALIDITY_NOT_AFTER,
12. IPOQUE_SSL_SERVER_HELLO_INVALID_SUBJECT_LEN

EDR will contain a value of 1-12 corresponding to above reasons in the same order with IPOQUE_SSL_CLIENT_HELLO_DECODE_SUCCESS being 1 and IPOQUE_SSL_SERVER_HELLO_INVALID_SUBJECT_LEN being 12.

Following are the conditions when above failure reasons will be reported:

- Client Hello Success – Client Hello decoded successfully but further packets are not received in flow (absence of Server Hello).
- Server Hello Success – SSL flow decoded successfully without any issues, both Client and Server Hello packets.
- Invalid Client/Server Hello Extension Length – When length of any of the TLVs in Client/Server Hello is 0 (zero) or more than packet length respectively.
- Server Hello No certificate – Absence of any certificates in Server Hello.
- Server Hello Invalid Subject/SNO/Signature Len – When length of Subject/Serial Number/Signature TLVs in Server Hello is 0 (zero) or more than packet length respectively.
- Server Hello Issuer Not Found – Absence of Issuer certificate in Server Hello.
- Server Hello Invalid Validity/Validity Not Before/Validity Not After – Absence of these fields in Server Hello.
- Subject Organization Name – Name of the Organization/Company to which the SSL certificate is issued.
- Issuer CNAME – Canonical Name of the Organization/Company issuing the certificate
- Issuer Organization Name – Name of the Organization/Company issuing the SSL certificate
- SSL Certificate Validity:
  - EDR value of 1 – Current date is less than Certificate not before date
  - EDR value of 2 – Current date is greater than Certificate not after date

- EDR value of 3 – Current date is within Certificate not before and not after dates

  Issuer provides a certificate subjected for a particular duration of time, after which the same must be renewed or the certificate is deemed invalid. This field states whether the certificate exchanged in Server Hello is currently valid or expired.

Configuring SSL Parameters in EDR

This section provides information on CLI commands available in support of this feature.

Enabling SSL Parameters

Use the following configuration to enable SSL Parameters under EDR Format Configuration Mode:

```
active-charging service service_name
  edr-format format_name
    rule-variable p2p ssl-params { cert-issuer-cname | cert-subject-oname
 | cert-issuer-oname | cert-validity | ssl-decode-failure } priority
priority
    end
```

NOTES:

- **ssl-params**: Specifies the SSL flow parameters.
- **cert-issuer-cname**: Specifies the SSL Certificate Issuer CName.
- **cert-subject-oname**: Specifies the SSL Certificate Subject Organization Name.
- **cert-issuer-oname**: Specifies the SSL Certificate Issuer Organization Name.
- **cert-validity**: Specifies the validity of SSL Certificate.
- **ssl-decode-failure**: Specifies the reason for SSL Decode failure.

Monitoring and Troubleshooting

This section provides information about show CLI commands and/or their outputs in support of this feature.

Show Commands and/or Outputs

show active-charging edr-format all

The output of this CLI command has been enhanced to display the new SSL parameters. Following is a sample output:

```
show active-charging edr-format all
 Service Name: service_1
  Edr Format  Name: edr_1
      rule-variable p2p ssl-params cert-subject-oname priority 1
```

show configuration active-charging service all

The output of this CLI command has been enhanced to display the new SSL parameters. Following is a sample output:

```
show configuration active-charging service all
config
  active-charging service service_1
    no ng-ecs-enabled
    edr-format edr_1
      rule-variable p2p ssl-params cert-subject-oname priority 1
    exit
    rulebase default
      no tcp check-window-size
    exit
    policy-control burst-size auto-readjust duration 5
  exit
end
```